Auditdienst Rijk
Ministerie van Financiën

Rapport over de Automatische Factuurcontrole in SAP M&F

Colofon

Audit Dienst Rijk
Cluster Geïntegreerde Bedrijfsvoering
Postbus 20201
2500 EE DEN HAAG

Contactpersoon

Kenmerk ADR/2014/1052

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

1 Samenvatting

1.1 Belangrijkste bevindingen

Het onderzoek naar de Automatische Factuurcontrole is gebeurd in het kader van de werkzaamheden die binnen de wettelijke controletaak worden uitgevoerd. Het doel van het onderzoek was bezien welke maatregelen zijn ingericht in Automatische Factuurcontrole in SAP en hoe deze bijdragen aan rechtmatig betalen. Daarbij was de insteek van het onderzoek gericht op het presenteren van feitelijke bevindingen.

De belangrijkste bevindingen zijn:
Documentatie is niet volledig en niet met elkaar in overeenstemming:

- Ontwerpdocumentatie is niet actueel;
- Ontwerpdocumentatie is niet zichtbaar vastgesteld door bevoegd gezag;
- In ontwerpdocumentatie zijn customizingsettings niet duidelijk aangegeven;
- Niet duidelijk is hoe procesmatig gezien besluitvorming rondom toleranties heeft plaatsgevonden met inachtneming van de Comptabiliteitswet.

Customizing in SAP wijkt af van ontwerp:

- Er zijn verschillen geconstateerd tussen instellingen in SAP en ontwerp in ARIS;
- Maatwerk en workflow beïnvloeden mogelijk de werking van geprogrammeerde controles in de customizing, onduidelijk is welk effect dit heeft;
- De uitgevoerde testen zijn zeer beperkt gedocumenteerd waardoor niet inzichtelijk is of kritieke procesaflopen zijn getest;

Autorisaties zijn te ruim ingesteld en monitoring daarop dekt niet het gehele spectrum af:

- Autorisaties zijn te ruim ingesteld waardoor functiescheiding wordt doorbroken;
- Monitoring van functiescheiding in rapportages vindt niet conform Key controls van HDFC plaats.

De bevindingen zijn mogelijk van invloed op aard en omvang van de overige werkzaamheden uit hoofde van de wettelijke controletaak.

2 Inleiding

2.1 Aanleiding opdracht

Op 19 mei 2014 is de Automatische Factuurcontrole (AFC) in SAP in produktie genomen. De AFC in SAP vervangt het handmatige verificatieproces bij het betaalbaar stellen van facturen. Het doel van verificatie (al dan niet geautomatiseerd) is zorgdragen voor de rechtmatigheid van betalingen. Deze ontwikkeling van handmatige naar geautomatiseerde controle is aanleiding voor dit onderzoek.

2.2 Scope

De afstemming van prijs en hoeveelheid op de factuur, order en levering is het object van onderzoek, alsmede de functiescheiding tussen besteller, ontvanger, agendeur/verificateur en autorisator.

Het onderzoek wordt beperkt tot de Application Controls c.q. de inrichting van SAP specifiek voor de AFC, inclusief bijbehorende afscherming (autorisaties) tot de AFC functionaliteit.

Procedurele maatregelen hebben we buiten de scope van het onderzoek geplaatst (usercontrols en rapportages). Specifiek wordt hierbij gedacht aan de mogelijkheid waarbij prestatieverklaringen voor goederenontvangst en diensten worden afgegeven zonder controle op juistheid, tijdigheid en volledigheid van de levering. Eveneens zijn buiten de scope de General IT-controls (Changemanagement en logische toegangsbeveiliging). We kijken naar de generieke inrichting in het systeem en niet naar de manier waarop de bedrijfsvoering met de three-way match omgaat.

Verder gaan wij bij dit onderzoek er vanuit dat:

- de Purchase Orders (PO) die in SAP zijn opgevoerd, rechtmatig tot stand zijn gekomen (op basis van autorisaties e.d.). De bestaande PO is het startpunt voor de match;
- de Goederen Ontvangsten (GO) die in SAP zijn opgevoerd, daadwerkelijk hebben plaatsgevonden;
- de registratie/boekingen van facturen in SAP heeft juist, tijdig en volledig plaatsgevonden.

3 Doel en aanpak opdracht

3.1 Doel

Het doel van de inrichting van automatische factuurcontrole door SAP is te bewerkstelligen dat facturen altijd rechtmatig worden betaald. Om te bezien in welke mate dit het geval is geven wij antwoord op de volgende vraag:

Welke maatregelen zijn ingericht in de Automatische Factuurcontrole in SAP M&F en hoe dragen deze bij aan rechtmatig betalen?

Het onderzoek naar de Automatische Factuurcontrole is onderdeel van de jaarrekeningcontrole van het Ministerie van Defensie.

Deze opdracht is uitgevoerd in opdracht van Clustermanager Defensie 3

3.2 Aanpak

Wij hebben onderzocht welke application controls in het SAP M&F systeem zijn genomen en welke zekerheden daaraan kunnen worden ontleend dat de automatische factuurcontrole om de rechtmatigheid van het automatisch vrijgeven van facturen te borgen.

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing.

De volgende documentatie is bestudeerd om dit onderzoek uit te voeren:
- Artikel 22 lid 1 van de comptabiliteitswet. Hierin is opgenomen: "Het Financieel beheer voldoet aan de eisen van rechtmatigheid, ordelijkheid en controleerbaarheid en wordt overigens zo doelmatig mogelijk ingericht";
- Ontwerpdocumentatie SAP M&F, welke is opgenomen in ARIS;
- Data Doel Sheets (DDS), die op Sharepoint staan;
- Functionele en Technische documentatie, welke is opgenomen in SAP Solution Manager;
- Documentatie die is overhandigd door de Projectcoördinator FINAD;
- Best practises ten aanzien van de inrichting van automatische factuurcontrole, welke zijn verkregen door interviews met EY.

Daarnaast zijn diverse mensen geïnterviewd om een toelichting te vragen over de problematiek van de AFC. Ook hebben we in SAP bezien welke settings zijn ingericht. Tenslotte heeft hoor wederhoor plaatsgevonden met projectcoördinator FINAD en zijn VBT-teamleden.

3.3 Verspreiding rapport

Deze rapportage wordt uitgebracht aan:

HDFC Directeur DIMB

4 Bevindingen

4.1 Documentatie is onvolledig en niet met elkaar in overeenstemming

Om te beoordelen of het ontwerp van de beoogde functionaliteit voldoende helder is beschreven om de customizing door te voeren hebben wij documentatie uit ARIS en Sap Solution Manager (SSM) bestudeerd. Reden hiervoor is dat ARIS de norm bevat van het ontwerp (SOLL) en SAP Solution Manager (SSM) bevat alle Request For Changes (RFC). In de RFC's behoren ondermeer de technische instellingen te zijn opgenomen. Daarnaast is er een Excel bestand bestudeerd dat we hebben ontvangen van Projectcoördinator FINAD met de besluiten rondom de tolerantie instellingen. Tenslotte zijn Data Doel Sheets (DDS) bestudeerd, in het bijzonder een embedded file waarin de motivatie opgenomen zou moeten zijn voor beantwoording van de vraag welke specifieke toleranties moeten zijn ingericht en het niveau daarvan.

In ARIS, waar het ontwerp van SAP is opgenomen, is nagegaan of de three way match maatregel is opgenomen. Deze maatregel is op 4 plekken opgenomen in: 3.3.08a act 010, 1.1.05 act 020, 1.1.06 act 010, 2.2.06 act 020.
Zowel in ARIS als in het functionele ontwerp (Functional Customizing Documentation "IMG Logistic Invoice - Set Tolerance Limits" versie 0-2-1) is beschreven welke tolerantiegrenzen ingesteld moeten zijn. Dit document geeft echter geen duidelijkheid over de andere mogelijk in te stellen toleranties in SAP. Daarnaast is er een Excel bestand ontvangen van Projectcoördinator FINAD met de besluiten rondom de tolerantie instellingen. Het embedded file in het DDS is niet up to date en motivatie is zeer beperkt opgenomen. We hebben vastgesteld dat deze bronnen niet met elkaar in overeenstemming zijn. Ook hebben wij niet kunnen vaststellen of een of meerdere van deze bronnen door bevoegd gezag is geautoriseerd.

In de comptabiliteitswet, art 22 lid 1, is opgenomen: "Het Financieel beheer voldoet aan de eisen van de rechtmatigheid, ordelijkheid en controleerbaarheid en wordt overigens doelmatig ingericht". Dit artikel heeft impact op de te kiezen toleranties in SAP. Enerzijds geeft dit artikel aan: tolerantie is nihil. Anderzijds ligt er de doelmatigheidsvraag. Dit is een nieuw aspect waar nog niet eerder over hoefde te worden nagedacht. Vanwege het belang hebben wij de verwachting dat er een zorgvuldig besluitvormingsproces aan ten grondslag ligt, waarbij bevoegd gezag de tolerantieniveaus accordeert. Wij hebben vergaderverslagen ontvangen over dit onderwerp, maar hierin zijn tolerantie instellingen niet specifiek benoemd. De vraag blijft daardoor bij ons bestaan hoe zorgvuldig besluitvorming is geweest bij de totstandkoming van de gekozen tolerantie instellingen en door wie deze zijn vastgesteld.

Wij hebben vastgesteld dat de functionele en technische ontwerpdocumentatie niet volledig beschrijft welke customizing-instellingen er moeten worden aangepast en waar deze instellingen zich in SAP bevinden. Daarnaast missen wij een motivatie waarom bepaalde keuzes al dan niet zijn gemaakt. Een voorbeeld van een vraag die hierbij speelt is de inrichting van leveranciersafhankelijke toleranties. Zie bijlage 4. In de documentatie treffen wij hier niets over aan, waardoor onduidelijk is of dit wel of niet moet zijn ingericht.
Een ander voorbeeld is de instelling om toleranties te activeren. Deze instelling hebben wij niet in de documentatie aangetroffen (zie bijlage 5). Deze instelling is mogelijk van invloed op de tolerantie-instellingen zoals opgenomen in bijlage 1.

Daarnaast hebben wij in de functionele en technische documentatie een beschrijving van maatwerk aangetroffen. Deze functionaliteit is zo technisch van aard, dat wij niet zonder aanvullende technische deskundigheid kunnen vaststellen of deze qua opzet en bestaan juist is. Daarnaast is in een interview aangegeven dat de workflow is aangepast, maar daarvan hebben wij geen beschrijving aangetroffen. Zowel maatwerk als workflow kan impact hebben op de werking van de geautomatiseerde factuurcontrole.

Door projectcoördinator FINAD is tijdens hoor- wederhoor aangegeven dat de verschillende documenten onderling in lijn zullen worden gebracht en dat in de documentatie de niet in gebruik genomen toleranties zullen worden opgenomen. Opdrachten zijn hiertoe al gegeven.

4.2 Customizing in SAP wijkt af van ontwerp

Customizing
Het beoordelen van de volledigheid van de customizing in SAP is niet goed mogelijk gebleken, omdat enerzijds eenduidig vastgestelde documenten ontbreken waarin de uit te voeren customizing-settings (volledig) zijn opgenomen. En anderzijds is er sprake van maatwerk en workflow die mogelijk de werking van de automatische factuurcontrole beïnvloedt. Zoals bij 4.1 beschreven, hebben wij maatwerk en de aanpassing van de workflow niet kunnen beoordelen.

Wij hebben de tolerantie-instellingen in kaart gebracht op basis van aangetroffen documentatie en best practice EY (SOLL) en vervolgens gekeken hoe dit is ingericht in SAP (IST). In bijlage 1 is een overzicht opgenomen waaruit blijkt dat er twee verschillen zijn tussen SAP en het ARIS ontwerp.

Door projectcoördinator FINAD is tijdens hoor- wederhoor aangegeven dat het ontwerp in ARIS juist is en mag worden gehanteerd in plaats van de eerder verstrekte spreadsheets met toleranties of andere bronnen. Overigens is het zo dat in de Business Control Diagrams uitsluitend die toleranties worden vastgelegd die ingericht moeten worden en niet de toleranties die toch niet worden gebruikt. Ten aanzien van best practices (tolerantie PP, B1 en B2) is door projectcoördinator FINAD aangegeven dat commerciële bedrijven andere toleranties hanteren dan overheden vanwege het kas- en verplichtingenstelsel en ander beleid met betrekking tot betaalgedrag. Zoals aangegeven bij 4.1 zullen alle gekozen toleranties worden gedocumenteerd en wordt daarmee de best practice voor Defensie vastgelegd.

Testen
Wij hebben verslagen van de uitgevoerde testen doorgenomen om te bezien of application controls zijn getest op goede werking. Er zijn wel unittestresultaten AFC aangetroffen waaruit blijkt dat tolerantie-instellingen zijn geverifieerd en goed bevonden. Ook hebben wij geconstateerd dat het maatwerk op gebied van de kwaliteitscontrole is getest en volgens de beschrijving is dit goed verlopen.
Tenslotte hebben wij unittestresultaten AFC aangetroffen waaruit blijkt dat met positietype 'service' en positietype ongelijk aan 'service' is getest en goed bevonden.

De scope van de gedocumenteerde tests is wel beperkt. Wij hebben geen resultaten aangetroffen waaruit blijkt dat veel voorkomende bestelsoorten (BSART) zijn getest. Voorbeelden hiervan zijn: [Normale bestelling], [bestelling loonbewerking], [Z001 Std Concurrentie st.], [Z002 Std Geen concurrentie st.], etc. Voor de niet geteste procesafwikkelingen is het risico aanwezig dat facturen direct in de betaalvoorstellijst terecht komen, zonder dat deze getoetst worden

door application controls. Hierdoor bestaat de kans op onrechtmatige betalingen omdat inhoudelijke toetsing van de rechtmatigheid van de betaling niet meer plaatsvindt.

De projectcoördinator FINAD heeft tijdens hoor-wederhoor aangegeven dat hij onze mening niet deelt. Hij geeft aan dat er een zeer uitgebreide test is uitgevoerd met meerdere invalshoeken en op verschillende momenten tijdens de implementatie, maar dat deze testen inderdaad niet volledig zijn gedocumenteerd. Dit was ook bekend bij de leider van het voortbrengingsteam. Alles overziend was dit geen blokkerende reden om toch de AFC te migreren naar Produktie.

Na livegang zijn de nodige maatregelen genomen om nog meer zekerheid te krijgen over de juiste en consistente werking. Zo worden wekelijks steekproeven verricht om te bekijken of ten onrechte facturen betaalbaar worden gesteld.

Procesafwikkeling
Om een indruk te krijgen van de procesafwikkeling in SAP hebben we bezien welke mogelijkheden daadwerkelijk zijn gebruikt. Daartoe hebben wij een download gemaakt van alle nieuwe bestellingen van 01.01.2014 - 18.05.2014. De resultaten zijn weergegeven in bijlage 3. De tabel geeft voor de verschillende bestelsoorten aan of er al dan niet een goederenontvangst en/of factuurontvangst is verwacht. Opmerkelijk is dat bij een aantal bestelsoorten de verwachte goederenontvangst en factuurontvangst van elkaar afwijken. Een voorbeeld hiervan is bestellingen loonbewerking. Bij 242 bestelregels wordt wel een goederenontvangst verwacht, maar slecht bij 78 bestelregels een factuur. Dit geeft aan dat het aanzetten van de vinken "factuurontvangst" en "goederenontvangst" niet is afgedwongen (zie bijlage 2 Rubriceringstypes en positietypes met GO en/of FO al dan niet verplicht).

De projectcoördinator FINAD heeft tijdens hoor-wederhoor aangegeven dat wekelijks de goede werking van de geprogrammeerde controles wordt gecontroleerd. Er is immers sprake van een overgangsperiode. 10% van het aantal facturen onder € 1.250,- en 20% van het aantal facturen > € 1.250,- wordt bezien op de juist werking van de AFC. Dit gebeurt sinds 19-5-2014 en zal op termijn moeten worden overgedragen aan medewerkers van FABK. Reden voor deze controle achteraf is dat de complexiteit van de elkaar beïnvloedende instellingen zo groot is dat niet met zekerheid kan worden gesteld dat de AFC altijd juist werkt. T/m 17/6 zijn er 837 facturen betaald waarbij vrijgave via de AFC heeft plaatsgevonden. Uit controle is gebleken dat tot 18 juni 2014 vrijgave steeds terecht heeft plaats gevonden.

4.3 Autorisaties te ruim ingesteld met negatieve impact op functiescheiding

In de impactanalyse van SSM 14602 versie V2 28-11-2011 is geen aandacht besteed aan functiescheiding en impact op rollen. Dit is opmerkelijk omdat er een nieuwe rol nodig is met inhoudelijk andere bevoegdheden. De nieuwe verificateurrol hoeft niet meer te controleren op rechtmatigheid (dat doet SAP) maar moet de factuur zowel registreren als boeken.

De projectcoördinator FINAD heeft tijdens hoor- en wederhoor aangegeven dat er geen sprake is van een nieuwe rol. Alleen de Workflow is aangepast waardoor functiescheiding wordt afgedwongen.
Hij geeft aan dat wellicht de suggestie is gewekt dat er sprake is van een geheel nieuwe rol. In de "volksmond" is dit ook het geval, namelijk verificateur AFC. Maar technisch blijft dit de bestaande verificateur omdat er sprake is van een transitie van huidige werkwijze (FI-proces) naar de nieuwe werkwijze (MM-proces). Op enig moment gaan alle aanwezige verificateurs hiermee werken. Door te werken met een specifiek toewijzing van een verificateur aan een

workflowbak (24) wordt geregeld dat momenteel de huidige 4 verificateurs AFC de MM-facturen kunnen afhandelen. Als het aantal MM-facturen toeneemt, kan heel flexibel het aantal verificateurs AFC worden uitgebreid.
Een tweede reden voor de nu gekozen oplossingsrichting is dat uitbreiding van een rol in SAP M&F extra beheerslast betekent voor Beheer.

In de PPC hebben wij de bevoegdheden van de verificateur opgezocht. Deze rol kan bij automatische factuurcontrole handmatig verschillen accepteren waardoor het risico ontstaat van onrechtmatige betalingen (zie bijlage 7). Deze bevoegdheid ligt niet in lijn met de werkzaamheden van de nieuwe rol. De verificateur mag alleen boeken wat er op de factuur staat en niet verschillen accepteren. Hier zou nader onderzoek naar verricht kunnen worden.

Met de kritieke transactie MRBR kunnen facturen handmatig worden vrijgegeven. Hierdoor kunnen blokkades door overschrijding van toleranties "overruled" worden. Uit bijlage 8 blijkt dat beheerders beschikken over MRBR op de Produktie omgeving. Hierdoor wordt functiescheiding doorbroken. Daarnaast hebben 14 functionarissen met de rol autorisator de bevoegdheid om deze kritieke transactie uit te voeren terwijl niet al deze functionarissen conform functie/afdeling een autoriserende bevoegdheid hebben. Hierdoor wordt de functiescheiding tussen bestellen, ontvangen en uiteindelijk betalen doorbroken.
Het handmatig vrijgeven van geblokkeerde facturen zouden wij willen beperken tot 2 personen of hooguit drie. Voor de CARIB mensen kunnen wij ons voorstellen dat alle drie deze mensen deze rol hebben i.v.m. continuïteit van het werk op de afdeling, maar gezien de taken, bevoegdheden en verantwoordelijkheden zouden logistieke mensen deze transactie niet mogen hebben.
Wij hebben nagegaan of in de afgelopen maanden MRBR is gebruikt. Dit bleek niet het geval te zijn.

Door projectcoördinator FINAD is tijdens hoor- wederhoor aangegeven dat de bevoegdheid voor MRBR bij beheerders op de produktieomgeving wordt ingetrokken. De aanpassing is inmiddels verricht en succesvol doorgevoerd op de productieomgeving op 9 juli 2014 om 15:27.

Functiescheiding tussen bestellen, ontvangen en betalen is als key control door HDFC gedefinieerd (bron: BPA betaalproces). Uit de CSI AA rapportage blijkt dat deze functiescheiding als geheel niet wordt gemonitord. Wel wordt functiescheiding in het financiële domein door HDFC gemonitord en in het Logistieke domein door DMO, echter het monitoren van het koppelvlak tussen het financiële en logistieke domein kan worden verbeterd. Dit is bevestigd in een interview.

Door projectcoördinator FINAD heeft tijdens hoor- wederhoor aangegeven dat de betreffende conflicten uit de MATLOG rapportage ook aan HDFC zullen worden aangeboden.

5 Appreciatie op hoofdlijnen / Aanbevelingen

5.1 Appreciatie Projectcoördinator FINAD

Tijdens hoor en wederhoor met de Projectcoördinator FINAD heeft hij zijn mening gegeven over de bevindingen.

- Naar aanleiding van de 1e hoor en wederhoor is door de projectcoördinator FINAD aan verschillende mensen gevraagd de ontwerpbronnen/documentatie met elkaar in lijn te brengen;

- Ten aanzien van testen geeft de projectcoördinator aan dat naar zijn mening zorgvuldig en uitvoerig is getest door deskundige mensen. Resultaten daarvan zijn naar zijn mening betrouwbaar en tonen de juiste werking aan.
  Niet alle uitgevoerde testen zijn volledig gedocumenteerd; met name bij acceptatietesten ontbreken testverslagen.

- De werking van de AFC wordt nu handmatig gemonitord. Iedere week voert een functionaris van het voortbrengingsteam (VBT) een deelwaarneming uit op de betaalde facturen. Vervolgens worden deze handmatig gecontroleerd om te borgen dat uitsluitend rechtmatige betalingen plaats vinden.

- De inrichting van autorisaties en monitoring daarop wordt aangepast. Autorisaties van beheerders zijn inmiddels ingetrokken en monitoring door HDFC wordt uitgebreid met functiescheidingsconflicten uit het MATLOG domein.

5.2 Aanbevelingen

Het doel is te komen tot een AFC die er voor zorgt dat facturen rechtmatig worden betaald. De AFC beperkt de noodzaak van usercontrols. Dit is effectief en efficiënt. De vraag is hoe dit bereikt kan worden zonder onacceptabele risico's te nemen.

Wij adviseren hiertoe de volgende stappen te ondernemen, met daarbij de opmerking dat er al door projectcoördinator FINAD acties in gang zijn gezet om de volgende aanbevelingen uit te voeren:

- Het ontwerp in ARIS, de funcionele en technische ontwerpdocumentatie in SSM en op Sharepoint (DDS) actualiseren;

- Laat de documentatie met betrekking tot de AFC in de volle breedte inzicht geven in instellingsmogelijkheden en de gemaakte keuzes. Dit geldt ook voor aangebrachte maatwerk en workflow;

- Tolerantie instellingen dienen alle gedocumenteerd te zijn en voorzien van gemotiveerde afweging van voorgeschreven waarden, en laat deze accorderen door het bevoegd gezag en bewaren op een centrale plaats;

- Tijdens het hoor en wederhoor is verschil van inzicht gebleken op het vlak van het uitvoeren van testen. Wij adviseren om in de toekomst testen goed

gedocumenteerd uit te voeren. Dit helpt het testproces te structureren waardoor het testproces beter beheerst verloopt en uiteindelijk onnodig herstelwerk achteraf voorkomt. Verder maakt het inzichtelijk welke testactiviteiten hebben plaatsgevonden.

- De handmatige controle (steekproefsgewijs) op betaalbaar gestelde / betaalde facturen aan te houden totdat de AFC aantoonbaar géén systematische fouten bevat. Controle op de werking van de AFC is nodig om eventuele onrecht-matige betalingen en problemen met de inrichting van AFC te signaleren. De inrichting van deze controle is nog nader te bepalen door HDFC in overleg met belanghebbenden;

- Op dit moment is de gebruikte rapportage om autorisaties te monitoren niet adequaat ingericht om functiescheidingsconflicten, die het MATLOG domein en het FINAD domein overstijgen, te identificeren. We adviseren de rapportage aan te passen zodanig dat autorisaties in ene domein die leiden tot mutatiees in het andere domein expliciet gepresenteerd worden. Hierbij in acht nemend dat functiescheiding in het betalingsproces een Key control vormt voor de HDFC. Daarnaast vinden wij dat het uitgifte van kritieke transacties zo beperkt mogelijk moet worden gedaan. Daarom adviseren wij een heroverweging van de uitgifte van de transactie MRBR, waarmee facturen betaal gesteld kunnen worden.

6 Ondertekening

Den Haag, 18 juli 2014

Projectleider ADR DEF1

Audit Dienst Rijk
Postbus 20201
2500 EE DEN HAAG
(070) 342 77 00